TRANSMITTAL SLIP	DATE

TO: ER

ROOM NO.	BUILDING

REMARKS:

Copies on distribution were hand carried.

FROM:

ROOM NO.	BUILDING	EXTENSION

FORM NO. 241 REPLACES FORM 36-8 WHICH MAY BE USED. (47)
1 FEB 55

ER 84-4047

19 July 1984

MEMORANDUM FOR: Information Systems Board Members

FROM: [redacted] 25X1
Executive Secretary to the Board

SUBJECT: Minutes of 29 June 1984 Meeting of the Information Systems Board

1. The Information Systems Board met on Friday, 29 June 1984 to consider computer security issues. [redacted] 25X1

[redacted] 25X1

2. [redacted] asked for approval of the minutes of the 25 May meeting. (Note: The Executive Secretary had received some corrections from [redacted] These changes were made and corrected copies were distributed at the meeting.) There were no other additions or corrections. [redacted] 25X1 25X1 25X1

3. [redacted] presented the two decision points the Computer Security Working Group had identified for the Board's consideration -- who determines "need-to-know" and who can waive the rules governing ORCON dissemination in an emergency. The Working Group has crafted a single "Inter-Agency Data Sharing Policy" and two recommendations for changes to DCID 1/7. He indicated that the policy and changes remain controversial, are not universally endorsed by the directorates or even by the members of the Working Group, and could cause fundamental changes in CIA's data sharing relationships both within the Agency and within the Community. [redacted] also briefly outlined the status of the RECON GUARD test, which is now being evaluated but appears to have been successful. [redacted] 25X1 25X1 25X1

4. [redacted] explained the proposed "need-to-know" and ORCON changes to DCID 1/7 and outlined the position of the DO -- that no changes should be made to DCID 1/7 other than strengthening the definition of "need-to-know" by changing the words "determination by an authorized holder" to "determination by the originator." (C) 25X1 25X1

DCI EXEC

[redacted]

5. [redacted] briefed the Board on the "Inter-Agency Data Sharing Policy." He noted that the draft policy was based on the assumptions that the Board had agreed to previously and that this draft policy, if approved, would require follow-on regulations for implementation. [redacted] 25X1 25X1

6. [redacted] thanked the Working Group for their efforts and reminded the Board that following its deliberations, EXCOM and eventually Community approval of the policy would be required. He noted that [redacted] Director of the Community's COMPUSEC Project, had called for a Community data-sharing policy. He said that the Agency needed to think seriously about the status of "need-to-know" and other security controls in a future of world-wide electronic data sharing, since near-real-time collection and disappearance of the boundary between tactical and strategic intelligence will cause increasing dissatisfaction among intelligence consumers. [redacted] 25X1 25X1 25X1

7. Beginning a general discussion of the Working Group's recommendations, [redacted] mentioned the pressure from Community members at the monthly Information Handling Committee meetings to better define "need-to-know" and ORCON. He predicted continued maneuvering in these areas, especially by those agencies which want to include CIA reporting in their automated data bases. [redacted] 25X1 25X1 and [redacted] agreed that the ORCON control was originally intended to protect the source, not necessarily the data, and that the receiving individual was responsible for proving "need-to-know," not the originator. [redacted] suggested separate controls for the source of the information and the actual data. [redacted] 25X1 25X1 and [redacted] argued that source and data were usually too intertwined to separate. [redacted] reminded the Board that the original purpose of DCID 1/7 was to govern the dissemination and sharing of data with those who needed it, not to restrict the information. [redacted] remarked that sources could be protected by rewriting the information, and that such a technique could be used more frequently, if needed. [redacted] 25X1 25X1 25X1 25X1 25X1 25X1 25X1

8. [redacted] began a discussion of the ORCON suggestions by reminding the Board of the difference between disseminating an original document and approving the use of data contained in that document for further publication. The ORCON controls were intended to cover both decisions, he said. [redacted] remarked that the originator cannot entirely control dissemination on paper, and rhetorically asked why the originator should expect more control from electronic dissemination. [redacted] remarked that DCID 1/7 was a compromise, giving each NFIB member the responsibility for control and protection within his agency or department. He pointed to the tendency periodically to overuse the ORCON control, citing studies which showed that the use of the ORCON label had increased from about 20 percent of DO disseminations in the mid-1970s to about 85 percent today. He suggested that the Agency must have informed evidence of the need for ORCON if it is to base data sharing decisions on the security argument. [redacted] 25X1 25X1 25X1 25X1

9. [redacted] then asked about the status of RECON GUARD wondering if it would "secure" Agency data bases sufficiently to 25X1

permit the on-line use of those data bases by other NFIB member agencies. [redacted] stated that OCR was still evaluating the results of the test on the prototype device and would need to test a real device further. [redacted] predicted that the Community will require the Agency to share its automated data bases sooner or later, and recommended that we be prepared for this eventually. [redacted] 25X1 25X1 25X1 25X1

10. [redacted] suggested that those opposing the proposed changes to the DCID might not oppose the milder wording of the "Crisis Imperative" section of the draft policy. [redacted] felt that the section on "Minimum Standards of Security" would leave the Agency open to problems if we chose not to disseminate information to agencies who admittedly met the "minimum security standards." [redacted] asked whether or not the Agency was prepared to let others set standards for us. [redacted] who is the CIA representative to the Community's computer security project, remarked that the standards must be geared to the policy they were intended to enforce, but that the policy must come first. He briefed the Board on the Community's efforts to establish standards, reminding them that policy or standards, the Community had to start somewhere. [redacted] asked for acceptance of the draft "Inter-Agency Data Sharing Policy" (attached) and approval to forward it to the Executive Committee. The Board concurred. [redacted] 25X1 25X1 25X1 25X1 25X1 25X1

11. [redacted] next suggested that the definition of "need-to-know" as currently contained in DCID 1/7 was adequate. The Board members concurred that no change would be proposed. Responding to a request for final comments on the recommended change to ORCON definition, [redacted] remarked that some users might find the new version more restrictive than the old. [redacted] agreed, noting that the military is already disseminating intelligence information as needed during periods of crisis. The Working Group's "Crisis Imperative" clause merely condones that which is already occurring, but adds the requirement to report back such dissemination which is not now done. Thus, we gain some damage control. [redacted] cautioned that the word "emergency" is too all-inclusive and that we need to better define what we mean by it. [redacted] agreed. The Board then voted to approve the proposed change and submit the new definition (attached) to the Executive Committee, excepting [redacted] representing the DO position. [redacted] 25X1 25X1 25X1 25X1 25X1 25X1 25X1

12. [redacted] thanked the Board members for their assistance and cooperation over the past year, and adjourned the meeting. The next meeting is scheduled for Thursday, 19 July, at 1100 hours in Room 7D64. (U) 25X1

[redacted] 25X1

Attachments

Distribution
1 - Compt
1 - D/OC
1 - D/ODP
1 - D/OIS
1 - D/OS
1 - D/OCR
1 - D/NPIC
1 - D/OD&E
1 - D/ORD
1 - D/OSO
1 - C/IMS
1 - C/ASG
1 - ER
1 - Planning Staff

[redacted]

25X1

Proposed Changed to ORCON Definition
(as contained in DCID 1/7, Page 4, Paragraph 2)

-- Information bearing this marking may not be disseminated in whole or in part through briefings, incorporation into reports, or in any other manner outside the headquarters elements* of the recipient organizations, or used in taking investigative action, without the advanced permission of, and under conditions specified by, the originator. During a National Emergency or an immediate physical threat to US military forces, installations, or civilians, the senior US official in the area threatened, at his discretion, can disseminate information bearing this marking to subcommands without advanced permission. The disseminating official must assume responsibility to protect the information and notify the originator of this action. As this is the most restrictive marking herein, agencies will establish procedures to ensure that it is only applied to particularly sensitive intelligence and that timely procedures are established to review requests for futher dissemination of intelligence bearing this marking. This marking may be abbreviated as "ORCON" or as "OC."

*At the discretion of the originator, the term "headquarters elements" may include specified subordinate intelligence-producing components.

4 June 1984

AN INTER-AGENCY DATA SHARING POLICY

PURPOSE. This policy establishes and describes conditions under which CIA data* can be shared with non-CIA individuals and organizations. All CIA officers of components that produce or provide initial or retrospective distribution of CIA data to non-CIA individuals or components must enforce this policy within the CIA.

BASIC PRINCIPLE. Data sharing is a necessary and positive function of intelligence work. Data sharing is driven by the "need to know" (NTK) principle, which requires that the CIA make available to policymakers, analysts, operations officers, and others, data that relates to the recipient's mission and function. Data sharing is limited, however, by the third agency rule and prudent security practices including: clearances, compartmentation, and protection of sources and methods. The NTK principle itself also requires that data not be shared with those who do not have a legitimate need.

COROLLARY I. Decisions to share--or not to share--data must be based on judicious balancing of NTK and other security considerations. A consistent policy mandates that such decisions not be capricious or arbitrary, nor should they be based on mindless standard operating procedures.

* Data is defined as any information, regardless of its form (bibliographic, full text, numeric, etc), length, age, or use. This policy addresses both classified data and unclassified data of a sensitive nature.

COROLLARY II. A distinction must be made between substantive data (intelligence information) and descriptions of sources or methods from which the intelligence information is derived. The mandate of NTK--to put relevant data in the hands of those who legitimately need it--may be satisfied by sharing only substantive data. Sources and methods data should also be shared but within the constraints of security access approvals, compartmentation regulations, and protection of sources and methods.

DECISIONMAKING. All data sharing decisions must be made within frameworks set by the DCI, DDCI, Executive Director, and the Deputy Directors. Any of these may delegate orally or in writing to their subordinates the power to decide whether data that originated within their authority should be shared. Similarly, they may prohibit the sharing of specific data or categories of data with any non-Agency individual or organization if that decision is in keeping with the spirit of this policy. In no case should an individual CIA officer share data with a non-CIA individual or organization unless that officer has at least tacit approval through the appropriate chain of command.

CRISIS IMPERATIVE. An immediate physical threat to US military forces, installations, or civilians, automatically generates a need to know by the senior US official in the area of the threat. In addition, when a clear and present danger to US military forces, installations, or civilians is reflected in intelligence data, that data must be shared expeditiously with the senior US official in command of the area. Standard operating procedures derived from this policy for non-crisis conditions must not prevent the sharing of data that will protect the lives of US citizens.

MINIMUM STANDARDS OF SECURITY. The CIA has minimum standards of security for information and communications systems. Agency officials will authorize and execute data sharing with non-CIA individuals and/or organizations only after receiving specific information that confirms that the transmission system and storage/access/use systems of the recipient meet the Agency's standards of security.** If any link in a transmission or storage/access/use system is unacceptably vulnerable in terms of the minimum standards, such systems must not be used for data sharing.

RECIPIENT ENFORCEMENT OF NTK. Before authorizing data sharing, Agency producers and distributors must acquire from recipients an oral or written description of recipient's procedures for enforcement of NTK that satisfies the producer or distributor that the data will be distributed in the recipient organization only to those with a legitimate need. CIA officers have no police power over other agencies; therefore, care must be taken in advance to ensure a pattern of compliance with NTK by recipients.

CIA SELECTIVITY. CIA officers must decide what data to share. The basic principle, however, cannot be arbitrarily or capriciously applied. Officers in other agencies who have a legitimate NTK must not be denied relevant data provided they adhere to minimum standards of security, comply with the principle of NTK as described herein, and will not as recipients pose an unwarranted risk to sources and methods.

**The word "systems" is used generically and includes automated or electronic as well as manual or hard copy methods. "Security" includes physical, technical, and procedural aspects of protecting data.

FAILURE OF ENFORCEMENT. CIA officers cannot directly enforce minimum standards of security, NTK, or protect sources and methods in recipient organizations. At any time, however, CIA can suspend data sharing with a recipient if it has reason to believe that the recipient of shared data is not enforcing agreed upon minimum standards of security and NTK within its system. A temporary suspension can become permanent if the recipient fails to satisfy minimum standards. If a temporary suspension becomes permanent, the officer authorizing the suspension must request Director of Security to investigate through OS contacts the infraction and must report the suspension to the DCI via the chain of command.

INITIAL SURVEY. Before data is shared, producers and distributors of data ~~become~~ will familiar with the needs, security systems and procedures, and uses for shared data by recipients. Recipients must be thoroughly briefed on the sensitivity and permitted use of the shared data (usually as described in DCID 1/7).

PERIODIC REVIEW. Data sharing, once instituted, must not be automatically continued. Both originators and recipients must periodically review all data sharing agreements, whether written or oral, to determine whether NTK continues, whether minimum standards of security continue to be applied, and whether undue risks to sources and methods occur. Such reviews should occur at least annually or more frequently if necessary.